

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-148156

(43)Date of publication of application : 29.05.2001

(51)Int.Cl. G11B 20/10
G06F 12/14
G06F 13/00
G11B 19/04
H04H 1/00
H04L 9/32

(21)Application number : 11-331932

(71)Applicant : NTT DATA CORP

(22)Date of filing : 22.11.1999

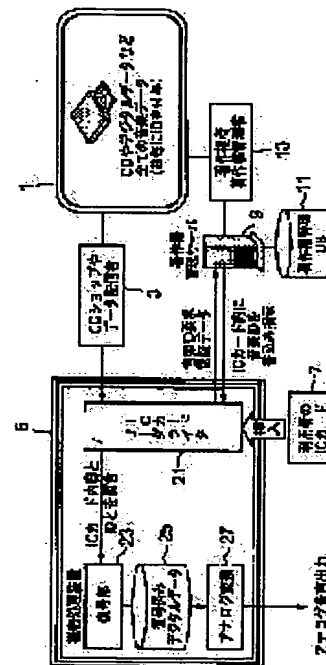
(72)Inventor : TAKAHASHI SHINJI

(54) SYSTEM AND METHOD FOR DISTRIBUTING AND USING DIGITAL CONTENTS

(57)Abstract:

PROBLEM TO BE SOLVED: To protect copyright about digital contents such as the music, images, texts and programs which are distributed widely.

SOLUTION: In regard to music, for example, all music data are generally sold via the CDs or a network with an ID given to every piece of music and after encipherment. A user, who purchases the music data must decode them via a secrecy processor 5, to reproduce music from the music data. The processor 5 contains an IC card reader/writer 21, collates a music ID given to the music data with a music ID included in an IC card 7 that is set by the user to recode the music data, only when both IDs are identical with each other. The music ID can be written on the card 7 only via a copyright management server 9, that is managed by a copyright owner 13. The owner 13 can monitor the copyright payment, etc., when the music ID is written on the card 7. The processor 5 will not output the recoded digital music data 25 to the outside and outputs only the converted analog music signals.



LEGAL STATUS

[Date of request for examination]

06.02.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(43)公開日 平成13年5月29日(2001.5.29)

(51)Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
			3 2 0 C
	13/00	13/00	3 5 4 Z
G 1 1 B 19/04	5 0 1	G 1 1 B 19/04	5 0 1 H
審査請求 有 請求項の数10 OL (全 6 頁) 最終頁に続く			

(21)出願番号 特願平11-331932

(22)出願日 平成11年11月22日(1999. 11. 22)

(71)出願人 000102728

株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号

(72)発明者 高橋 真次

東京都江東区豊洲三丁目3番3号 株式会社エヌ・ティ・ティ・データ内

(74) 代理人 100095371

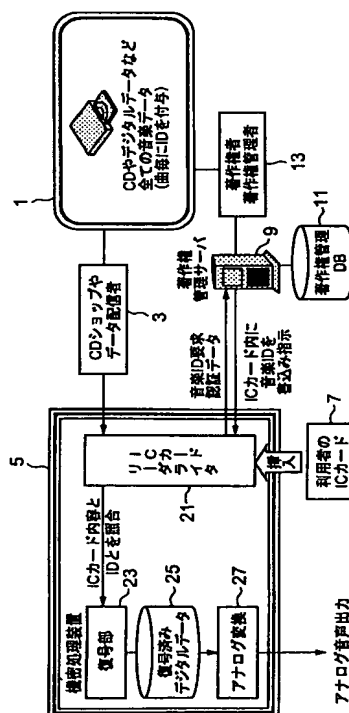
弁理士 上村 輝之

(54)【発明の名称】 デジタルコンテンツの配布・利用方式及び方法

(57) 【要約】

【課題】 広く配布される音楽、映像、テキスト、プログラムなどのデジタルコンテンツについての著作権を守る。

【解決手段】 例えば音楽の場合、全ての音楽データ１は、楽曲毎のＩＤを付され、暗号化した状態でＣＤ又はネットワークを通じて一般に販売される。音楽データを購入したユーザが、その音楽データから音楽を再生するには、機密処理装置５による復号化を必要とする。機密処理装置５は、ＩＣカードリーダライタ２１を内蔵し、音楽データの復号化の際、音楽データに振られた楽曲ＩＤと、ユーザがセットしたＩＣカード７内の楽曲ＩＤとを照合し、同じＩＤがあるときだけ復号化を行う。ＩＣカード７内に楽曲ＩＤの書込みをすることは、著作権者１３の管理下におかれた著作権管理サーバ９だけが可能である。著作権者１３は、ＩＣカード７への書込みの際に、著作権料支払いなどについて監視を行うことができる。機密処理装置５は、復号化したデジタル音楽データ２５を機密処理装置５の外には出さず、変換したアナログ音楽信号のみを出力する。



【特許請求の範囲】

【請求項 1】 暗号化されたデジタルデータと、このデジタルデータのコンテンツについての利用権チェック用コードとのセットを配布するためのデータ配布媒体と、前記データ配布媒体から前記暗号化されたデジタルデータと前記利用権チェック用コードを受け取り、また、前記コンテンツについての利用権をもつ者のみが取得可能な利用権証明用コードをユーザからの入力によって受け取り、前記利用権チェック用コードと前記利用権証明用コードとから、前記ユーザが前記コンテンツについての利用権をもつか否かを判断し、この判断結果が肯定の場合に前記暗号化されたデジタルデータを復号化し、この復号化したデジタルデータから前記コンテンツを再生する機密処理装置と、を備えたデジタルコンテンツの配布・利用方式。

【請求項 2】 前記ユーザは、前記利用権証明用コードを記憶するための記憶装置を所持し、この記憶装置を前記機密処理装置に接続することによって、前記利用権証明用コードを前記機密処理装置に入力する請求項 1 記載のデジタルコンテンツの配布・利用方式。

【請求項 3】 前記記憶装置が IC カードである請求項 2 記載のデジタルコンテンツの配布・利用方式。

【請求項 4】 前記ユーザに対して特定のコンテンツについての利用権を与えて良いか否かを判断し、この判断結果が肯定の場合に前記ユーザに対して前記特定のコンテンツについての前記利用権証明用コードを提供する管理サーバを更に備え、

前記ユーザは、前記特定のコンテンツについての前記利用権証明用コードを取得するために、前記管理サーバにアクセスしなければならない請求項 1～3 のいずれか一項記載のデジタルコンテンツの配布・利用方式。

【請求項 5】 前記ユーザは、前記機密処理装置に接続できる IC カードを所持し、前記管理サーバは、前記ユーザの IC カードにネットワークを通じて又は直接的に前記利用権証明用コードを書き込むことにより、前記ユーザに前記利用権証明用コードを提供する請求項 4 記載のデジタルコンテンツの配布・利用方式。

【請求項 6】 前記機密処理装置が、前記復号化したデジタルデータを前記機密処理装置の内部でのみ使用して前記機密処理装置の外部には漏らさない請求項 1 記載のデジタルコンテンツの配布・利用方式。

【請求項 7】 暗号化されたデジタルデータと、このデジタルデータのコンテンツについての利用権チェック用コードとのセットをユーザに配布するステップと、機密処理装置が、前記ユーザに配布された前記暗号化されたデジタルデータと前記利用権チェック用コードを受け取るステップと、前記機密処理装置が、前記コンテンツについての利用権をもつ者のみが取得可能な利用権証明用コードをユーザ

からの入力で受け取り、この利用権チェック用コードと、前記ユーザに配布された利用権証明用コードとから、前記ユーザが前記コンテンツについての利用権をもつか否かを判断するステップと、前記機密処理装置が、前記判断の結果が肯定の場合に、前記暗号化されたデジタルデータを復号化し、この復号化したデジタルデータから前記コンテンツを再生するステップと、を備えたデジタルコンテンツの配布・利用方式。

【請求項 8】 ユーザに配布された暗号化されたデジタルデータと、このデジタルデータのコンテンツについての利用権チェック用コードとのセットを受け取る手段と、前記コンテンツについての利用権をもつ者のみが取得可能な利用権証明用コードをユーザ入力する手段、前記受け取った利用権チェック用コードと前記ユーザ入力された利用権証明用コードとから、前記ユーザが前記コンテンツについての利用権をもつか否かを判断し、この判断結果が肯定の場合に前記暗号化されたデジタルデータを復号化し、この復号化したデジタルデータから前記コンテンツを再生する手段とを備えたデジタルコンテンツを再生する機密処理装置。

【請求項 9】 前記利用権証明用コードをユーザ入力する手段が、前記利用権証明用コードを記憶した IC カードに接続して、この IC カードから前記利用権証明用コードを読み込む手段を有する請求項 9 記載の機密処理装置。

【請求項 10】 ユーザに配布された暗号化されたデジタルデータと、このデジタルデータのコンテンツについての利用権チェック用コードとのセットを受け取る手段と、前記コンテンツについての利用権をもつ者のみが取得可能な利用権証明用コードをユーザ入力する手段、前記受け取った利用権チェック用コードと前記ユーザ入力された利用権証明用コードとから、前記ユーザが前記コンテンツについての利用権をもつか否かを判断し、この判断結果が肯定の場合に前記暗号化されたデジタルデータを復号化し、この復号化したデジタルデータから前記コンテンツを再生する手段とを備えたデジタルコンテンツを再生する機密処理装置として、コンピュータを機能させるためのプログラムを担持したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】本発明は、デジタルコンテンツ（デジタルデータ化された音楽、映像、テキスト、プログラムなどのコンテンツ）を記録ディスクやネットワーク信号などに載せて人々に配布し利用に供するためのデジタルコンテンツの配布・利用方式に関わり、より詳しくは、コンテンツに係る著作権等の権利を確実に保護

できるようにするためのデジタルデータ処理技術に関する。

【0002】

【従来の技術】例えば音楽を例にとると、従来、音楽の著作権使用料は、音楽媒体（例えば、コンパクトディスク（CD）やカセットテープなど）の提供者、もしくは音楽放送者に対して、CDやテープの販売本数や販売額に見合った額を徴収することにより達成されてきた。

【0003】しかし、最近では、音楽の利用方法が多岐にわたり、従来の管理方法では困難な局面がでてきた。例えば、デジタルデータ化された音楽データをインターネットで配信する場合である。この場合、データ配信した数量の把握が重要となるが、それはデータ配信者の申請に頼る他なく、これでは確実な方法とはいえない。

【0004】この問題に対して、音楽データの暗号化等を用いて著作権保護を行おうとする提案がなされた。例えば、特開平07-131452号のものは、共通鍵で暗号化されたデータを、機密処理部内で復号化して開くというものである。この場合、配信先の共通鍵に合わせてデジタルデータを暗号化するのであれば、音楽データは配信先の者以外利用できないため、著作権管理がかなり正確に出来る。

【0005】

【発明が解決しようとする課題】しかし、特開平07-131452号のものは、購入したCDをデジタルデータとしてインターネット上に公開するなどの方法に対しては無防備である。現在最大の問題は、個人が購入したCDを勝手にデジタルデータ化して、インターネット上に公開することにより、著作権者の権利が侵害されていることである。この点について対策を行う事が必要である。

【0006】従って、本発明の目的は、勝手にCDデータをコピーして配信するような不正行為を防ぎ、デジタルコンテンツについての権利を守ることができるデジタルコンテンツの配布・利用方式を提供することにある。

【0007】

【課題を解決するための手段】本発明に従うデジタルコンテンツの配布・利用方式は、暗号化されたデジタルデータと、このデジタルデータのコンテンツについての利用権チェック用コードとのセットを配布するためのデータ配布媒体と、このデータ配布媒体から前記暗号化されたデジタルデータと前記利用権チェック用コードを受け取り、また、前記コンテンツについての利用権をもつ者のみが取得可能な利用権証明用コードをユーザからの入力によって受け取り、前記利用権チェック用コードと前記利用権証明用コードとから、前記ユーザが前記コンテンツについての利用権をもつか否かを判断し、この判断結果が肯定的場合に前記暗号化されたデジタルデータを復号化し、この復号化したデジタルデータから前記コンテンツを再生する機密処理装置とを備える。

【0008】なお、上記データ配布媒体には、CDのよ

うな固体の記録媒体のほか、通信ネットワーク信号などの様々な形態の情報伝達媒体が含まれる。

【0009】このシステムによれば、配布されたデジタルデータは暗号化されているので、そのままではコンテンツを再生することができない。そして、利用権証明用コードを取得した者のみが、そのデジタルデータを復号化してコンテンツを再生することができる。従って、コンテンツの著作権者等の側で、利用権証明用コードのユーザへの提供を適正に管理すれば、個々のユーザ単位でコンテンツにかかる著作権料の徴収などを的確に行うことができる。

【0010】ユーザが自己の利用権証明用コードを機密処理装置に入力する方法として、好適な実施形態では、ユーザが自己の利用権証明用コードを記憶するための記憶装置を所持し、この記憶装置を機密処理装置に接続することによって、自己の利用権証明用コードを機密処理装置に入力する。この方法によれば、一般のユーザは、コンテンツを再生するためにその記憶装置を接続することが必要だということを知るだけで、そこに記憶されている利用権証明用コードを知ることはない（利用権証明用コードの存在自体にも気付かないであろう）。よって、配布されたデジタルデータが大量にコピーされて出回っても、利用権を持たない不特定多数者がデジタルコンテンツを再生する可能性は低く安全である。

【0011】好適な実施形態では、上記記憶装置としてICカードを使う。ICカードは、複製が困難で機密保持性が高く且つ内部のデータ改竄も困難であるから、ICカードを用いることで、上述したコンテンツの安全性は非常に高くなる。

【0012】好適な実施形態では、個々のユーザに対しユーザ所望のコンテンツについての利用権を与えて良いか否かを判断し、この判断結果が肯定的場合にそのユーザに対してそのコンテンツについての利用権証明用コードを提供する管理サーバが、コンテンツの著作権者等の権利者の管理下に設けられる。各ユーザは、入手したデジタルデータのコンテンツについて、管理サーバにアクセスして、その利用権証明用コードを取得しなければ、入手したデジタルデータからコンテンツを再生することができない。これにより、著作権者等の権利は、正当なユーザ（例えば、デジタルデータの購入証明を持つユーザ）だけに利用証明用コードを与えることができるので、個々のユーザ単位でコンテンツにかかる著作権料の徴収などを的確に行うことができる。

【0013】好適な実施形態では、前記管理サーバは、ユーザの持つICカードに通信ネットワークを通じて又は直接的に利用権証明用コードを書き込むという方法で、ユーザに利用権証明用コードを提供する。そのため、ユーザに利用権証明用コードを知られることなく、コンテンツの利用権管理を安全に行うことができる。

【0014】好適な実施形態では、機密処理装置は、復号化した後のデジタルデータを、機密処理装置の内部でのみ使用して、機密処理装置の外部には漏らさない。これにより、復号化したデジタルデータが不法にコピーされて出回るという虞がなくなる。

【0015】

【発明の実施の形態】本発明の一実施形態の構成と動作を示すブロック図である。

【0016】この実施形態は、音楽のデータ配布と利用のためのものであるが、この実施形態の説明から、当業者は映像、テキスト、プログラムなどの他のコンテンツの配布と利用のための実施形態について理解できるはずである。

【0017】1曲又は複数曲の音楽を表したデジタルデータ（音楽データ）1が、予め暗号化された状態で用意されている。この暗号化された音楽データ1には、各楽曲毎の識別コード（以下、音楽IDという）が付加されている。この暗号化され且つ音楽IDとセットになった音楽データ1は、例えば音楽CDに記録されていたり、或いは、例えばウェブサーバに記憶された状態で存在している。

【0018】音楽データの配布業者（例えば、CDショップ業者やネットワーク配信業者）3は、上記音楽CDをユーザに販売したり、或いは、ウェブサーバから通信ネットワークを通じて上記音楽データをユーザのコンピュータに配信したりする。こうしてユーザに提供された音楽データは、暗号化されているので、そのままでは音楽を再生することはできない。

【0019】ユーザは、上記音楽データを復号化して音楽を再生するための機密処理装置5を持っている。また、ユーザは、ICカード7を所持している。機密処理装置5は、汎用のデジタルコンピュータを用いて実現されてもよいし、或いは、専用の装置として作られていてもよいし、或いは、汎用デジタルコンピュータに搭載された機能拡張回路として実現されていてもよい。この機密処理装置5は、ICカードリーダライタ21を備えていて、そこにユーザがICカード7をセットすれば、そのICカード7にアクセスすることができる。また、この機密処理装置5は、通信ネットワークを通じて、音楽著作権を管理するための著作権管理サーバ9にアクセスすることができる。この機密処理装置5の機能と動作の詳細は後に説明する。

【0020】著作権管理サーバ9は、上記のようにしてユーザに配布された音楽データに含まれる楽曲に係る著作権を、その著作権者又は著作権管理者（以下、著作権者等という）13に代わって管理するためのコンピュータシステムである。この著作権管理サーバ9は、著作権管理データベース11を有しており、このデータベース11は、上記音楽データに付加されたのと同じ各楽曲の音楽IDを保持している。著作権管理サーバ9がもつ

つの機能は、ユーザの機密処理装置5から通信ネットワークを通じて、特定の楽曲に係る音楽IDの要求を受けると、当該ユーザが当該楽曲を聴く正当権利をもっているか否かを判断し、その判断結果が肯定であれば、当該楽曲の音楽IDを通信ネットワークを通じて当該ユーザの機密処理装置5へ送信して、その音楽IDのICカード7への書き込みを当該機密処理装置5に許可（又は指示）することである。また、この著作権管理サーバ9がもつ別の機能は、各楽曲の音楽IDについて、それをユーザに提供した履歴（例えば、提供した数量（ユーザ人数又は提供回数など）や、提供した日付など）を著作権管理データベース11に蓄積して、著作権者等13から要求があったとき又は定期的になど必要に応じて、その提供履歴を著作権者等13に報告することである。

【0021】以下、ユーザのもつ機密処理装置5の機能と動作について詳しく説明する。

【0022】機密処理装置5は、前述した著作権管理サーバ9との通信機能及びICカードリーダライタ21の他に、音楽CDや通信ネットワークから読み込んだ暗号化された音楽データを復号化するための復号部23と、復号化された音楽データ25をアナログ音楽信号に変換してアナログ音声を出力する（つまり、音楽を再生する）アナログ変換部27とを備える。

【0023】ユーザは音楽CDを購入しただけ、又はウェブサーバから正当に音楽データをダウンロードしただけでは、そこに入っている音楽を再生することはできない。更に、ユーザは、自分のICカード7を機密処理装置5のICカードリーダライタ21にセットした上で、機密処理装置5から著作権管理サーバ9にアクセスし、購入した音楽CD又はダウンロードした音楽データに入っている楽曲の音楽IDを、著作権管理サーバ9から機密処理装置5に送ってもらって、その音楽IDをICカード7に書き込んでおく必要がある。この音楽ID提供処理を行うときには、機密処理装置5から著作権管理サーバ9へ、要求対象の楽曲を指定した音楽IDの要求と、ICカード7が正当なものであることを証明するための認証データを送る。すると、著作権管理サーバ9は、受け取った認証データからICカードが正当か否かを判断する装置認証を行う。加えて、著作権管理サーバ9は、要求対象の楽曲に係る音楽データをユーザが正当に購入したかどうか、つまり、ユーザがその音楽データの正当な利用権者か否かを判断するための利用権認証も行う。その結果、装置認証と利用権認証の双方が成功したときのみ、著作権管理サーバ9は、要求された楽曲の音楽IDを機密処理装置5に送信して、機密処理装置5に対しその音楽IDをICカード7に書き込むことを許可（又は指示）する。

【0024】ここで、上記した利用権認証は、例えば次のような方法で行う。

【0025】（A）音楽CDなどの媒体で音楽データ

を販売する場合、CDショップ内のマシンから、購入者のICカード7へ、CDショップのデジタル署名付き領収書などの購入証明データを書き込む。ユーザは、上記利用権認証を行う際、ICカード7内の購入証明データを、機密処理装置5から著作権サーバ9へ送信し、著作権サーバ9は受け取った購入証明データに基づいて利用権認証を行う。或いは、CDショップ内のマシンから著作権管理サーバ9へ、購入者のICカード7の識別情報と販売した楽曲の識別情報とを送信し、著作権サーバ9は、装置認証を行うとき、CDショップ内のマシンから受け取った上記識別情報と、ユーザの機密処理装置5から受け取った音楽ID要求及びICカード7の識別情報とから、楽曲とICカード識別情報の双方について一致するか否かで判断する。

【0026】(B) インターネットのウェブサーバなどから音楽データの配信を受けた場合は、あおのウェブサーバから、配信先の機密処理装置へ、配信元のデジタル署名付き領収書などの購入証明データを送信して、そのユーザのICカード7へ書き込む。ユーザは、上記利用権認証を行う際、ICカード7内の購入証明データを、機密購入者のICカード7へ処理装置5から著作権サーバ9へ送信し、著作権サーバ9は受け取った購入証明データに基づいて利用権認証を行う。

【0027】以上のようにして、ユーザのICカード7に楽曲の音楽IDが格納されると、機密処理装置5は初めて、購入した音楽データから音楽を再生することが可能になる。すなわち、ユーザは、購入した音楽を聴きたいとき、機密処理装置5のICカードリーダーライタ21に、自分のICカード7をセットした上で、機密処理装置5に対して音楽を再生が命じる。すると、機密処理装置5は、ICカード7から音楽IDを読み込み、その読み込んだ音楽IDと、再生対象の音楽データに付されている音楽IDとを照合し、一致するか否かを判断する。その結果、ICカード7内の音楽IDの中に、再生対象の音楽データの音楽IDと一致したものがあれば、機密処理装置5内の復号部23が作動して、その音楽データ（暗号化されている）の復号化を行う。復号化されたデジタル音楽データ25は、機密処理装置5内の記憶装置に一旦保持される。その後、機密処理装置5内のアナログ変換部27が、復号済みデジタル音楽データ25を、アナログ信号に変換してアナログ音声として出力する。

【0028】ところで、機密処理装置5内に保持された復号済みデジタル音楽データ25は、機密処理装置5の外部に取り出すことは絶対にできない。機密処理装置5

の外部へ出力され得るのは再生されたアナログ音声信号だけである。これにより、復号済みデジタル音楽データ25を複製して他の装置で利用することが禁止される。

【0029】上記のシステムによれば、次のような利点が得られる。

【0030】(A) 楽曲の音楽IDが書き込まれているICカードがないと、その音楽の再生ができず、且つ、ICカードは偽造困難なので、実質的にICカード所有者本人しか音楽を再生できず、よって、正当に購入していない不特定多数人によって自由に音楽が再生される虞が解消される。

【0031】(B) 音楽IDが書き込まれているICカードを持っている正当権利者なら、車の中でも、他人のオーディオ機器でも、該当する楽曲を聴くことができる。

【0032】(C) 音楽データは暗号化された状態で配布され、そのままでは聴くことができないので、どんなに大量にコピーして配布しても問題ない。

【0033】(D) ICカードへの音楽IDの書込みは、著作権者等を代理する権限のある機関しか行えないので、誰がどの曲を買ったか、明確に把握でき、著作権者等は著作料支払などを確実に管理できる。

【0034】以上、本発明の一実施形態を説明したが、これは本発明を説明するための例示であり、本発明は別の形態でも実施することができる。例えば、音楽に限らず、映像、テキスト、プログラムなど様々なコンテンツについても本発明が適用できる。著作権管理サーバでの認証の方法として、上に例示した方法以外にも様々な方法が採用し得る。

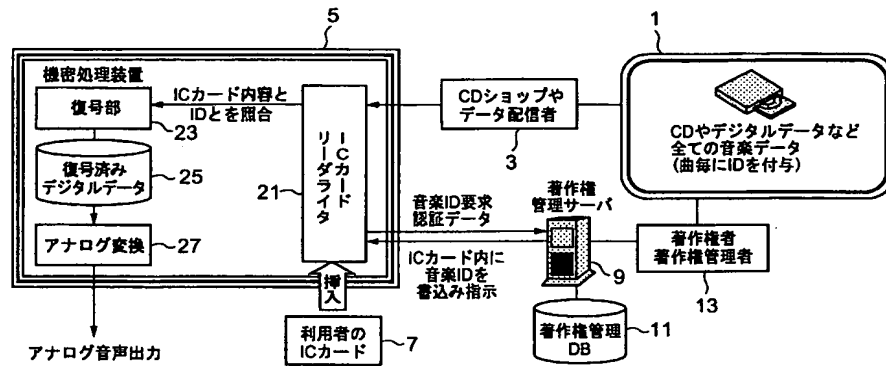
【図面の簡単な説明】

【図1】 本発明の一実施形態の構成と動作を示すブロック図。

【符号の説明】

- 1 暗号化された音楽データ
- 3 音楽データの配布業者（CDショップ業者やネットワーク配信業者）
- 5 機密処理装置
- 7 ICカード
- 9 著作権管理サーバ
- 11 著作権管理データベース
- 13 著作権者又は著作権管理者（著作権者等）
- 21 ICカードリーダーライタ
- 23 復号部
- 25 復号化された音楽データ
- 27 アナログ変換部

【図1】



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

テーマコード* (参考)

H 0 4 H 1/00

H 0 4 H 1/00

E

H 0 4 L 9/32

H 0 4 L 9/00

6 7 3 E

6 7 3 A